Jarkko Hyytiäinen

Vahva käyttäjätunnistus etäyhteyksissä

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikan koulutusohjelma
Opinnäytetyö
26.4.2011

Metropolia

Tiivistelmä

Tekijä(t) Otsikko Sivumäärä Aika	Jarkko Hyytiäinen Vahva käyttäjätunnistus etäyhteyksissä 36 sivua 26.4.2011
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja(t)	vanhempi konsultti Jussi Perälampi yliopettaja Janne Salonen

Tämän työn tavoitteena oli luoda tiivis katsaus vahvaan käyttäjätunnistukseen etäyhteyksissä. Työssä esitellään yleisimmät loppukäyttäjien etäyhteysratkaisut. Vahvan käyttäjätunnistuksen osalta esitellään kolme tunnisteluokkaa (jotakin käyttäjän tietämää, jotakin käyttäjän hallussa olevaa, jokin käyttäjän piirre tai ominaisuus) ja niihin liittyvä vahvan käyttäjätunnistuksen määritelmä.

Työn tuloksena on saatu raportti, jonka avulla asiaa ennalta tuntemattoman ihmisen on helppo saada perustietous aiheesta. Lisäksi käytännön osuudessa on esitetty käytännössä toteutettuna yksi vahvan käyttäjätunnistuksen ratkaisu etäyhteysratkaisuun liitettynä. Käytännönratkaisun rakentaminen osoitti teknisen toteutuksen olevan verrattain helppoa. Ratkaisu on ollut testikäytössä, ja se on todettu toimivaksi.

Vahvan tunnistamisen määrittely ja suunnittelu osoittautuivat haastavaksi tehtäväksi. Lisäksi esitetty avoimen lähdekoodin ratkaisu osoittautui yrityskäytön kannalta rajoittuneeksi muun muassa loppukäyttäjien salasanageneraattorien luomisen kannalta. Kokonaisuutena vahvan tunnistuksen ymmärtäminen ja toteuttaminen vaativat tätä työtä syvällisempää asiaan perehtymistä.

Avainsanat	vahva käyttäjätunnistus, kertakäyttösalasana, etäyhteys, OTP, VPN

Metropolia

Abstract

Author(s) Title Number of Pages Date	Jarkko Hyytiäinen Strong Authentication in Remote Access Solutions 36 pages 26 April 2011
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Data networks
Instructor(s)	Jussi Perälampi, Senior Consultant Janne Salonen, Principal Lecturer

This bachelor thesis was written for getting a brief consistent description about strong authentication for remote access solutions. The theoretical part begins by explaining the most used remote access solutions for end-users. Strong authentication is defined according to three authentication factors (something you know, something you have, something you are).

The result of the thesis is a description of strong authentication and remote access solutions for someone who is not yet familiar with these concepts. In the practical part of the study, one solution for implementing such a solution in practice is presented. Implementation turned out to be rather an easy task. The implementation has been tested and it has proved to be fully functional.

Defining and planning strong authentication seems to be a hard task. In addition, the presented open source based solution is troublesome as for enterprise use. Especially the provisioning password generator software for end-users is not easy enough to perform. For getting deep understanding and being able to plan and implement strong authentication successfully requires additional research.

Keywords	strong authentication, one time password, remote access solutions, OTP, VPN

Sisällys

1 Johdanto 1

2 Yleisimmät etäyhteystekniikat loppukäyttäjille 3

2.1 Tarve suojatuille etäyhteyksille 3
2.2 Tekniikoista 5
2.2.1 IPSec 5
2.2.2 SSL VPN 6

3 Vahva käyttäjätunnistus etäyhteyksissä 10

3.1 Perinteiset salasanat 11
3.2 Kertakäyttösalasanat ja varmenteet 14
3.3 Biometriset tunnisteet 15
3.4 Katsaus markkinoilla oleviin vahvan käyttäjätunnistuksen tuotteisiin 17
3.5 RSA SecurID 17
3.6 Uhkakuvat 20

4 Vahva käyttäjätunnistus MOTP-AS-ohjelmistolla toteutettuna 23

4.1 Microsoft Unified Access Gateway 2010 23
4.2 MOTP-AS 24
4.3 Toteutettu ympäristö 28
4.4 Toiminnallisuus 28

5 Päätelmät 31

5.1 Saavutetut tulokset 31
5.2 Työn ulkopuolelle rajatut kehityskohteet 32
5.3 Tulosten hyödynnettävyys 32

Lähteet 34

Lyhenteet ja käsitteet

application translation	SSL VPN -yhteyden ominaisuuksien laajennus, jossa sovelluksen tietoliikennettä kuljetetaan tunneloituna olemassa olevan yhteyden sisällä.
brute force	Salauksiin kohdistuva "raa-an voiman" hyökkäysmetodi, jossa käydään läpi järjestelmällisesti salausavaimen (tai käyttäjän salasanan) eri vaihtoehtoja tavoitteena löytää käytetty salausavain.
CRL	Certificate Revocation List, listaus kumotuista varmenteista, joiden käyttöä ei enää sallita.
IP	Internet Protocol, protokolla jota käytetään tietoliikennepakettien toimittamisessa perille pakettikytkentäisessä tietoliikenneverkossa.
IPSec	IP Security Architecture, joukko protokollia Internet-yhteyksien suojaamiseen.
kertakäyttösalasana	Salasana, jonka kohdejärjestelmä hyväksyy vain kerran.
man-in-the-middle hyökkäys	Hyökkäys jossa hyökkääjä asettuu asiakkaan ja palvelun väliin esittäytyen asiakkaalle palveluna ja pääsee täten suojatun yhteyden sisälle asiakkaan huomaamatta.
network extension	SSL VPN -yhteyden ominaisuuksien laajennus, jossa asiakkaalle tarjotaan haluttaessa rajoittamaton pääsy kohdeverkkoon.
OCSP	Online Certificate Status Protocol, protokolla jota käytetään mahdollisen varmenteiden voimassaolon kumoamistiedon välittämiseen. OCSP:llä saavutetaan CRL-listoja ajantasai-

	sempi tilanne. Lisäksi siirrettävän tiedon määrää on mahdollista pienentää, etenkin pitkiin CRL-listoihin verrattuna.
OTP	One Time Password, katso kertakäyttösalasana.
PKI	Public Key Infrastructure, julkisen avaimen hallintajärjestelmä.
proxy	Välityspalvelin, välittää, muokkaa ja suodattaa liikennettä asiakkaan ja palvelimen välillä. Toimii sovellustasolla ja mahdollistaa liikenteen oikeanmukaisuuden tarkistamisen sovelluskerroksessa.
RADIUS	Remote Authentication Dial In User Service, protokolla käyttäjätunnistuspalveluiden toteuttamiseen.
SSL	Secure Sockets Layer, salausprotokolla Internet-tietoliikenteen suojaamiseksi.
symmetrinen salaus	Salausmenetelmä, jossa samaa salausavainta käytetään sekä tiedon salaamiseen, että salauksen purkamiseen.
TLS	Transport Layer Security, edelleen kehitetty versio SSL:stä, voidaan käyttää nimityksenä SSL-versioille alkaen 3.1:stä.
token	Itsenäinen laite, joka sisältää tai tuottaa varmentamiseen käytettävää tunnistetietoa kuten kertakäyttösalasanoja.
varmenne	Luotetun tahon allekirjoittama todiste, jolla varmistetaan varmenteen esittäjän tunnistetiedot.
VPN	Virtual Private Network, tapa muodostaa osallistujien suhteen rajattu ja haluttaessa suojattu verkkoyhteys.

VPN-yhteyskäytävä	Yksittäinen osoite jonka kautta tarjotaan VPN-yhteys, katso VPN.
yksisuuntainen tiiviste	Matemaattinen funktio, jolla lähdedatasta voidaan tuottaa tunniste, josta ei pystytä palauttamaan lähdedataa.

1 Johdanto

Tämän työn tarkoituksena on tehdä selvitys yleisesti käytössä olevista vahvan käyttäjätunnistuksen menetelmistä loppukäyttäjien etäyhteyksiin liittyen. Aiheenvalinnan taustalla on oma työnkuvani Trusteq Oy:ssä, jossa rooliini kuuluu muun muassa pääsynhallinnan konsultointi. Niin ikään aiheen tekee ajankohtaiseksi tietotyössä alati korostuva muutos kohti liikkuvampia työtapoja, jonka myötä työpisteeseen sidottu pääsy yrityksen verkon resursseihin ei enää ole yksinään riittävä.

Teoriaosuudessa esitellään yleisimpiä tapoja julkaista turvallisesti yrityksen sisäverkon palveluja ja sisältöä rajatulle käyttäjäkunnalle. Asioita pyritään käsittelemään käytännönläheisesti keskittyen eri vaihtoehtojen eroihin käytössä. Tässä selvityksessä ei ole tarkoitus käydä läpi ratkaisujen taustalla olevaa tekniikkaa syvällisesti, vaan sitä käsitellään vain oleellisten erojen esiintuomiseksi ja kokonaiskuvan muodostamiseksi.

Käytännön osuus alkaa lyhyellä esittelyllä Microsoftin Unified Access Gateway 2010 -tuotteesta. Tämän jälkeen luodaan kyseisellä tuotteella julkaisu pohjaksi varsinaiselle käytännön toteutukselle, jossa kokeillaan vahvaa käyttäjätunnistusta. Vahva käyttäjätunnistus toteutetaan avoimen lähdekoodin MOTP-projektin tuottamien ohjelmistojen varaan, joilla pystytään toteuttamaan kertakäyttösalasanaan pohjautuva käyttäjätunnistus. Palvelinpäässä hyödynnetään MOTP-AS-ohjelmistoa ja käyttäjille tarjotaan salasanojen luomiseksi Java-pohjainen älypuhelimeen asennettava työkalu.

Trusteq on suomalainen tietoturvaan erikoistunut konsulttiyritys. Trusteq auttaa asiakkaitaan riskien ja yritysmaineen hallinnassa käyttäjätietoturvan ja pääsynhallinnan palvelujen avulla. Trusteq antaa asiakkailleen myös IT-infrahankkeiden projektijohdon palveluja.

Koska nykyään lähes kaikkien yritysten liiketoimintaan liittyvät tietojärjestelmät ovat tietoverkoissa, Trusteqilla on avainrooli asiakkaidensa liiketoiminnan jatkuvuuden, häiriöttömyyden ja säädöstenmukaisuuden varmistajana.

Trusteq tarjoaa asiakkailleen valmisohjelmistoja, konsultointia, koulutusta ja teknisiä tukipalveluja. Trusteqin avulla organisaatiot voivat järjestää henkilöstönsä, kumppaneidensa ja muiden tärkeiden sidosryhmiensä pääsyn tietojärjestelmiin helposti, hallitusti ja turvallisesti.

2 Yleisimmät etäyhteystekniikat loppukäyttäjille

Etäyhteysratkaisun käyttöönotto on tekniseltä toteutukseltaan yksinkertaisimmillaan melko suoraviivaista. Onnistuneeseen projektiin kuuluu kuitenkin paljon muutakin ja kokonaisvaltainen elinkaariajattelu vaatii huolellista suunnittelua jo ennen käyttöönottoa. Yrityksen sisäisen päätöksenteon kannalta käyttäjätunnistus on hankala erityisesti, koska tietoturva ei useimmiten ole yritystoiminnan kannalta tuottavaa. [1.]

Ensimmäinen vaihe on vaatimusten määrittely. Heti alussa on syytä määrittää, mitä luotavalta ratkaisulta odotetaan ja miten näitä odotuksia lähdetään toteuttamaan. Toinen vaihe on varsinaisen ratkaisun suunnitteleminen. Tässä vaiheessa on oleellista valita tekninen ratkaisu ja suunnitella sen vaatimat yksityiskohdat. Tieturvaratkaisuja suunnitellessa on tunnettava järjestelmiin kohdistuvat uhkat, joita vastaan ratkaisulla pyritään suojautumaan. Hyökkäysmetodit on syytä tuntea, ja ne tulee ottaa huomioon suunnitteluvaiheessa. Tämän jälkeen voidaan lähteä toteuttamaan testausvaihetta. Huolellisen testaamisen jälkeen voidaan tehdä päätös mahdollisesta tuotantoon siirtymisestä. Varsinainen käyttöönotto tulee tehdä porrastettuna hallittavissa kokonaisuuksissa. Onnistuneen käyttöönoton jälkeen ratkaisu siirtyy ylläpidettäväksi. Ylläpidon aikana ratkotaan mahdollisia ongelmia ja seurataan järjestelmän toimintaa. Mahdolliset tulevat muutokset käynnistävät prosessiin uudelleen. [2.]

Tässä työssä käsitellään lähinnä suunnittelu- ja testiympäristön toteutusvaiheita. Työn lähtökohtana ei ole selkeää käyttöönottoprojektia, vaan tarkoituksena on kartoittaa teknisiä ratkaisuja ja esitellä yksi niistä käytännössä. Painopiste on vahvassa tunnistamisessa, mutta kokonaiskuvan saamiseksi tutustutaan myös VPN-ratkaisuihin (Virtual Private Network).

2.1 Tarve suojatuille etäyhteyksille

Yhteistä erilaisille suojatuille etäyhteysratkaisuille on tarve muodostaa turvallinen tiedonsiirtokanava Internetin tai muun julkisen verkon yli. Tarve tämän tyyppiselle suojaukselle on kasvanut erityisesti Internetin johdosta. Internet tarjoaa laajasti saatavilla olevan kustannustehokkaan yhteysmuodon. Näin ollen on houkuttelevaa käyttää Inter-

nettiä siirtotienä, kunhan tietoturva pystytään pitämään riittävällä tasolla järkevin kustannuksin. [3.]

Verkkoliikenteen tunneloimisella pyritään suojautumaan tietojen paljastumista ulkopuolisille ja tiedon tahallista muuttamista vastaan. Lisäksi oleellista on mahdollisuus varmistua tahosta, jonka kanssa yhteys muodostetaan. Tiedon suojaaminen vaikeuttaa samalla myös verkkoliikenteen analysointia. Verkkoliikenteen määrää ei voida piilottaa, mutta yhteyden lopulliset osapuolet, varsinaisen siirretyn tiedon määrä ja tiedon sisältö voidaan halutessa suojata. [3.]

Verkkoliikenteen suojaamiseen on olemassa useita eri ratkaisuja. Suojausta voidaan toteuttaa ohjelmisto-, siirto-, verkko- tai datayhteystasoilla. Ohjelmistotason suojaus vaatii suojauksen huolellisen toteuttamisen jokaisen suojattavan ohjelmiston sisään. Tämä tekee ohjelmistotason suojauksesta työlään ja virhealttiin. Vastaavasti datayhteystasolla tehty suojaus soveltuu lähinnä yksittäisten verkkoyhteyksien suojaamiseen erikoistapauksissa. Näistä poiketen siirtokerroksessa tehty suojaus pystyy suojaamaan kerralla yksittäisen istunnon päätelaitteiden välillä. Verkkokerrokseen kohdistuva suojaus kykenee suojaamaan kaiken verkkoliikenteen ja on siten varsin salliva yhteensopivuuden näkökulmasta.

Edellä esitetyistä käytännönsyistä johtuen verkon tunnelointi toteutetaan useimmiten joko siirto- tai verkkokerroksessa. Näistä lähtökohdista tässä työssä käsitellään lähinnä näitä toteutuksia. Yleisimmin verkkokerroksessa käytetty tekniikka on IPSec (IP Security Architecture), jota käsitellään kappaleessa 2.2.1. Vastaavasti siirtokerroksen yleisin toteutustekniikka on SSL/TLS (Secure Sockets Layer, Transport Layer Security), jota käsitellään kappaleessa 2.2.2. [4.]

Yleisimmät loppukäyttäjän etäyhteystarpeet voidaan jakaa useimmiten kahteen eri ryhmään. Ensimmäisessä asetelmassa käyttäjä käyttää joko yrityksen hallitsemaa ja hänen käyttöönsä antamaa päätelaitetta tai hänen itse hallitsemaa päätelaitetta. Nämä lähtökohdat mahdollistavat tarvittavien ohjelmistojen asentamisen laitteelle. Näin ollen haluttaessa koneelle voidaan erillisillä ohjelmistoilla luoda mahdollisuus avata suojattu VPN-tunneli kulloinkin tarvittavaan kohdeverkkoon. Tämän ratkaisumallin etuna on mahdollisuus tarjota käyttäjälle käyttökokemus, joka vastaa suoraa kytkeytymistä ky-

seiseen verkkoon. Käytännössä VPN-tunnelin läpi on mahdollista sallia kaikki yleisimmin käytössä olevat yhteysmenetelmät ja siten pääsy kohdeverkkoon erittäin laajasti. Kappaleessa 2.2.1 esitellään IPSec pohjainen VPN-tunnelointi, joka on tyypillinen tapa toteuttaa esitetty ratkaisu.

Toinen yleisimmistä tilanteista poikkeaa edellisestä lähtökohdiltaan. Tässä tapauksessa loppukäyttäjä käyttää päätelaitetta, joka ei ole käyttäjän eikä etäkäytettäviä palveluita hallitsevan tahon hallinnassa. Näin ollen kyseiselle laitteelle ei välttämättä ole mahdollista asentaa yllä esitellyssä ratkaisumallissa tarvittavia erikoisohjelmistoja. Tarvitaan siis ratkaisu, joka toimii päätelaitteelta useimmiten valmiiksi löytyvin perustyökaluin. Tällaisen mahdollisuuden tarjoaa selaimen kautta toteutettu SSL VPN -tunnelointi. Tälle ratkaisulle on tyypillistä yhteyden vaivaton jakelu. Toisaalta selaimen läpi toteutettu SSL VPN -tunneli on rajoittuneempi verrattuna erillisellä ohjelmistolla toteutettuun. Perustoiminnallisuutena SSL VPN -tunnelin läpi julkaistaan selainpohjaisia palveluita. SSL VPN -ratkaisuja käsitellään luvussa 2.2.2. Asiakaskoneella suoritettavilla komponenteilla SSL VPN -yhteyden ominaisuuksia pystytään laajentamaan oleellisesti.

2.2 Tekniikoista

2.2.1 IPSec

IPSec on yksi ensimmäisistä VPN-yhteyksissä käytetyistä salaustekniikoista. Se on julkaistu vuonna 1995. Sen ongelmana olivat pitkään kovat laitteistovaatimukset. Nykyisillä laitteistoilla lisääntyneen laskennan merkitys on kuitenkin vähentynyt. Lähellä laitteistoa tapahtuva salaus on etu, koska tällaisella toteutuksella ohjelmiston ei tarvitse ottaa kantaa prosessiin. [5.]

IPSec-protokollan mukainen tiedon tunnelointi ja salaus tapahtuu verkkokerroksessa. Se mahdollistaa kaiken IP-pohjaisen (Internet Protocol) liikenteen tunneloinnin ilman, että käytettävien ohjelmien tarvitsisi erikseen tukea VPN-yhteyksiä. Lisäksi myös IP-paketin otsikkotiedot jäävät salatun paketin sisään ja kuuluvat siten suojauksen piiriin. Vastaavasti IPSec VPN -tunnelointi ei tarjoa joustavaa mahdollisuutta rajata suojausta vain yksittäisiin sovelluksiin. [4.]

IPSec tarjoaa mahdollisuuden toteuttaa kuusi yhteyttä turvaavaa piirrettä. Siirrettävä tieto voidaan suojata ulkopuolisilta tahoilta salauksella. Tiedon eheys voidaan taata tarkistussumalla. Yhteyden muodostavat päätelaitteet pitävät huolen siitä, että tietävät, minkä tahon kanssa yhteys on muodostettu. Yhteys on suojattu monistushyökkäyksiä (replay) vastaan. Salattua dataa on huomattavasti vaikeampaa analysoida, eikä siitä voi päätellä tietoa siirtäviä tahoja tai tiedonsiirron tiheyttä eikä siirretyn tiedon määrää. Lisäksi IPSec tukee pääsynhallintaa, jolla voidaan rajoittaa pääsy tiettyihin resursseihin vain halutulle käyttäjäryhmälle. [4.]

Tietoturvan kannalta IPSec-yhteys on mahdollista suojata yrityksen sisäisen PKI-järjestelmän (Public Key Infrastructure) tuottamilla varmenteilla. Tällä menettelyllä on saavutettavissa tarkasti tunnettu sertifikaattien hallinta. Toisaalta IPSec VPN -yhteyden luominen edellyttää aina päätelaitteelle asennettavaa ohjelmistoa. Yhteyden muodostamiseen tarvittava ohjelmisto saattaa löytyä valmiina joistain käyttöjärjestelmistä, mutta silloinkin koneelle täytyy asentaa tunnistukseen käytettävä konevarmenne. Tämä lisää ylläpidon työkuormaa ja vaatii hallitut päätelaitteet.

2.2.2 SSL VPN

SSL VPN on siirtokerrokseen sijoittuva VPN-tekniikka. SSL VPN on IPSec VPN:ään verrattuna joustavampi ja monipuolisempi. Se on tuettuna useimmissa nykyaikaisissa selaimissa, eikä siten vaadi perustoiminnallisuuden osalta erillisten ohjelmien asentamista. Se sallii myös huomattavasti hienojakoisemman rajauksen suojattavien sovellusten ja yhteyksien suhteen. Lisäksi sillä on mahdollista toteuttaa laajennettu SSL VPN, joka vastaa tietyiltä ominaisuuksiltaan IPSec VPN:ää. IPsec ja SSL VPN eivät kuitenkaan ole toisensa korvaavia ratkaisuja vaan soveltuvat hieman erilaisiin tarpeisiin. [2.]

SSL VPN voidaan toteuttaa kolmella eri loogisella toimintaperiaatteella. Kevein toteutus on niin sanottu ”proxy”. Tässä tapauksessa välityspalvelin (proxy) esittäytyy asiakkaalle tavoiteltuna palveluna ja hoitaa asiakkaan tietämättä keskustelun taustapalvelun kanssa. Yleisin tapaus on web-sivuston julkaisu välityspalvelimen läpi. Toinen vaihtoehto on niin sanottu ”application translation”. Sitä käytetään julkaistaessa sovelluksia, jotka eivät itsessään tue tiedonsiirtoa Internetin välityksellä. Nyt paitsi palvelinpäässä, myös asiakkaan päässä tarvitaan välityspalvelinta. Sen roolina on tulkita ohjelmiston tiedonsiirto Internetiin soveltuvaksi ja palauttaa se jälleen sovelluksen ymmärtämään muo-

toon. Laajin vaihtoehto on toteuttaa laajennettu tunnelointi (network extension). Tämä vaatii asiakasohjelmiston asentamista, jonka jälkeen tunnelointi voidaan laajentaa käsittämään yleisesti asiakkaan ja VPN-yhteyskäytävän välinen liikenne. [2.]

Periaatteessa SSL VPN on toteuttavissa ilman asennettavia ohjelmistoja ja se on siten joustava yhteyden muodostamiseen käytettävien koneiden suhteen. Koneella ajettavilla lisäosilla on kuitenkin saavutettavissa merkittäviä etuja. SSL VPN -yhteydet tukevat yleisesti päätelaitteen turvatarkastusta. Tämä ominaisuus mahdollistaa päätelaitteen tunnistamisen ja määriteltyjen vaatimusten mukaisuuden tarkastamisen. [2.]

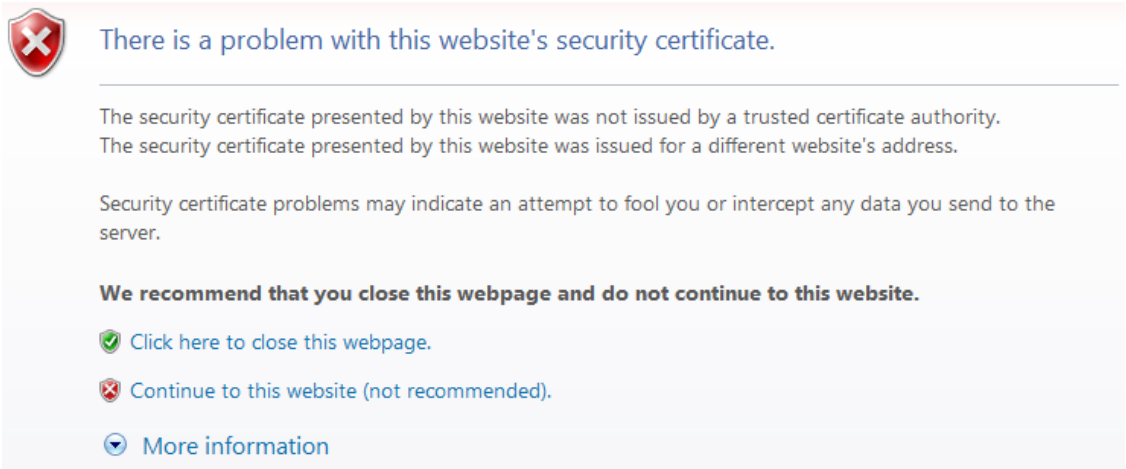
Päätelaitteen tunnistamisella on mahdollisuus erotella yrityksen hallinnassa olevat laitteet muista päätelaitteista. Näin ollen osalle laitteista voidaan halutuissa rajoissa sallia laajemmat käyttöoikeudet (enemmän sovelluksia tai vaikkapa pidemmät aikakatkaisurajat). Vastaavasti voidaan rajoittaa esim. yleisessä käytössä olevien kioskikoneiden osalta arkaluontoiseksi määriteltyjen palveluiden käyttämistä. [2.]

Edelleen sallittuja sovelluksia ja yhteyteen sovellettavia määrityksiä voidaan hallita päätelaitteen tietoturvatarkastuksen perusteella. Tässä tarkastuksessa asiakaskone raportoi SSL VPN -palvelimelle muun muassa käyttöjärjestelmäversion, asennetut tietoturvapäivitykset, käytettävissä olevan palomuurin ja virustorjunnan ajantasaisuuden. Näiden tietojen perusteella voidaan etukäteen määriteltyjen säännöstöjen perusteella valita millaisia ominaisuuksia kyseiselle asiakaskoneelle sallitaan. Lisäksi tietoturvaa voidaan parantaa siivoamalla automaattisesti yhteyteen käytetyn selaimen välimuisti yhteyden katkaisemisen jälkeen. [2.]

Suurimmat ongelmat SSL VPN -yhteyksissä liittyvät luottosuhteisiin ja sovellusten yhteensopivuuteen. Ehkä suurimman ongelman muodostavat useat eri selaimet, joilla asiakas voi yrittää yhteyden muodostamista. SSL VPN -ratkaisut tarjoavat vaihtelevan tuen eri selainversioille ja käytölle esimerkiksi matkapuhelimista. Myös tuki yhteyden yli julkaistavissa oleville sovelluksille on rajallinen. Kaikki sovellukset eivät toimi ainakaan ilman laajennettua VPN-tunnelointia. Se puolestaan vaatii aina asiakaskoneelle asennettavia laajennuksia, joita ei kaikissa tapauksissa ole mahdollista asentaa. Muutoinkin on syytä suhtautua kriittisesti mainoslauseisiin SSL VPN:ään riippumattomuudesta asennettaville sovelluksille. [2.]

Päätelaitteiden tietoturvatarkastukseen liittyy lisäksi omat ongelmansa. Tietoturvatarkastus voidaan määrittää pakolliseksi, mutta vastaukseen luottaminen on arveluttavaa. Ei ole olemassa keinoa varmistua siitä, ettei asiakaskoneella oleva haittaohjelma ole väärentänyt vastausta tai onnistunut huijaamaan tarkistusta. Yleisesti yhteyksien tarjoaminen hallitsemattomille koneille tarkoittaa, ettei asiakaskoneen tunnistamiseen ole käytettävissä mitään varmaa keinoa (kuten yrityksen itse allekirjoittamaa konevarmennetta). Samoin asiakkaan luottamus palvelimeen on kyseenalaistettavissa. Palvelin tunnistetaan julkisten varmenteiden perusteella ja niihin liittyy omat riskinsä (joita käsitellään luvussa 3.2).

Ongelmalliseksi voi muodostua myös SSL VPN -palvelimen vaatima varmenne. Tämän varmenteen perusteella asiakas voi tunnistaa keskustelevansa haluamansa (luottamuksen arvoisen) tahon kanssa. Yhteys voidaan kuitenkin julkaista myös itse allekirjoitetulla varmenteella. Kaikki toimii oikein niin pitkään, kun kaikille yhteyttä käyttäville päätelaitteille saadaan määriteltyä luottosuhde itse luotuun varmenteeseen. Ongelmalliseksi tilanne muodostuu, jos yhteyttä yritetään käyttää päätelaitteelta, joka ei luota käytettyyn varmenteeseen. Tällöin esimerkiksi selaimella portaaliin pyrkiessä käyttäjä saa varoituksen (esitetty kuvassa 1) varmenteeseen liittyvistä ongelmista.



Kuva 1. Varoitus varmenteeseen liittyvistä ongelmista

Käyttäjä voi hyväksyä varmenteen siihen liittyvistä ongelmista huolimatta. Yhteyden avaamisen kannalta järjestely on toimiva ja käyttäjä saa yhteyden käyttöönsä. On kuitenkin syytä huomata, että käyttäjän on vaikeaa, ellei mahdotonta havaita mahdollisesti käynnissä oleva palveluun kohdistuva hyökkäys. Erityisen vaaralliseksi tilanne muo-

dostuu, jos järjestely on pysyvä ja käyttäjiä ohjeistetaan ohittamaan varoitus. Tällöin riskinä on, että käyttäjä oppivat ohittamaan varmenteisiin liittyvät varoitukset yleisesti. Tällaisessa tilanteessa on heikennetty oleellisesti käyttäjien tietoturvaa paitsi oman, myös kaikkien muiden palveluiden osalta.

3 Vahva käyttäjätunnistus etäyhteyksissä

Vahva käyttäjäntunnistus ei ole terminä yksiselitteinen. Kaksi yleisintä määritelmää liittyvät joko tunnistetiedon välittämiseen tai käytettäviin tunnistetietoihin. Myös muita määritelmiä esiintyy lähteestä riippuen.

Ensimmäisen määritelmän mukaisesti vahva käyttäjäntunnistus tarkoittaa käyttäjän tunnistamista ilman, että varsinaista tunnistetietoa siirretään tietoverkon yli [6]. Tällä tarkoitetaan menettelyä, jossa toinen osapuoli voi todistaa tuntevansa ennalta sovitun salasanan lähettämättä tätä tunnistetietona. Tässä työssä ei käsitellä tämän määritelmän mukaista vahvaa tunnistamista.

Toinen tapa vahvan käyttäjätunnistuksen määrittelyyn on kuvata menettely, jossa tunnistaminen perustuu vähintään kahteen erityyppiseksi määriteltävään tunnistetietoon. Määritelmän mukaan tunnistetiedot jaetaan kolmeen eri ryhmään (suluissa on esitetty esimerkkinä yksi ryhmään luokiteltavista tunnisteista):

- jotakin käyttäjän tietämää (salasana)
- jotakin käyttäjän hallussa olevaa (tunnistekortti)
- jokin käyttäjän piirre tai ominaisuus (sormenjälki). [7.]

Kahteen erityyppiseen tunnisteeseen pohjautuvaa käyttäjätunnistusta pidetään lähtökohtaisesti vaikeampana murtaa verrattuna yhteen tunnisteeseen. On kuitenkin syytä huomioida, ettei kahden saman ryhmän tunnisteen käyttämistä tulkita vahvaksi tunnistamiseksi. Näin ollen esimerkiksi salasanan vahvistaminen PIN-koodilla ei täytä vaadittuja tunnusmerkkejä. Sen sijaan esimerkiksi yleisesti käytössä oleva ratkaisu yhdistää luottokortti ja PIN-koodi on selvästi vahvan käyttäjätunnistuksen tunnusmerkit täyttävä menettely. [7.]

Vahvan käyttäjätunnistuksen suunnittelu lähtee samoista lähtökohdista, kuin tietoturvaratkaisujen suunnittelu yleisemminkin. Erityishuomioita on syytä kiinnittää riskianalyysiin. Riski tulee suhteuttaa muun muassa tunnistettavan käyttäjän tyypin, tunnistuksen myötä sallittavien oikeuksien, käsiteltävän informaation luottamuksellisuuden ja

käytettävän yhteystyypin mukaisesti. Yleisemmällä tasolla huomiota tulee kiinnittää kerroksittaiseen suojautumiseen, eli tietoturvaan ja suojautumismekanismeihin tulee kiinnittää huomiota muuallakin kuin vain etäyhteysratkaisun käyttäjätunnistuksessa. [7.]

3.1 Perinteiset salasanat

Käyttäjätunnus ja staattinen salasana ovat erittäin laajasti käytössä oleva yhdistelmä käyttäjän tunnistamiseen. Tässä yhdistelmässä käyttäjätunnus kertoo käyttäjän identiteetin ja salasanaa käytetään tunnisteena identiteetin vahvistamiseen. Niihin pohjautuvaa tunnistamista käytetään paitsi kirjautumisessa erilaisille päätelaitteille (kuten työasemille), myös erittäin laajasti mitä erilaisimmissa palveluissa. Staattinen salasana muistuttaakin käyttöominaisuuksiltaan pitkälti perinteistä mekaanista avainta. Ehkäpä oleellisin ero avaimen ja salasanan välillä on ero käyttöalueessa. Avain käy usein vain muutamiin oviin, ja avaimen käyttäjän täytyy olla fyysisesti lukon luona. Salasanaa sen sijaan voi käyttää useimmiten lähes mistä vain ja pahimmillaan sama salasana on käytössä useissa eri järjestelmissä ja palveluissa.

Vertaus salasanan ja perinteisen avaimen välillä on perin osuva myös väärinkäytösten kannalta. Avaimien jättämisen yleisesti saataville koetaan yleisesti aiheuttavan ongelmia. Salasanan tapauksessa tilannetta pahentaa salasanan levittämisen helppous. Tahallisesti tai tahattomasti tapahtunutta salasanan leviämistä on lisäksi oleellisesti vaikeampaa havaita, koska tässä tapauksessa ei ole vastinetta fyysisesti kadonneelle avaimelle. Tämä on myös oleellisin ero vertauksen kannalta. Salasana ei ole jotain fyysisesti käytättäjän hallussa olevaa vaan jotain käyttäjän tietämää [10].

Staattisen salasanan heikkous tulee esiin ulkopuolisen tahon pyrkimyksessä tahallisesti saada haltuunsa hänelle kuulumaton salasana. Salasanat ovat erityisen houkuttelevia kohteita hyökkäyksille, koska nykyisessä toimintamallissa salasanoja vaihdetaan verrattain harvoin ja ne eivät ole erityisen monimutkaisia. Niinpä ne ovat alttiita jopa yksinkertaisimmille hyökkäyksille, kuten niin sanotulle ”brute force” -hyökkäykselle, eli salasanavaihtoehtojen järjestelmälliselle läpikäynnille. Lisäksi käyttäjillä on tyypillisesti tunnuksia useisiin eri palveluihin Internetissä. Tämä muodostuu ongelmaksi erityisesti koska varsin moni käyttäjä käyttää samaa salasanaa useissa eri palveluissa. Näin ollen mahdollisuudet hyökkäyksiin salasanaa kohtaan ovat jo lähtökohtaisesti laajemmat ja

lisäksi yksi heikosti tietoturvansa toteuttanut taho vaarantaa kerralla useita palveluja. [8.]

Internet mahdollistaa luonteensa takia helposti laajaan kohderyhmään kohdistetut hyökkäykset. Tämä näkyy käytännössä erilaisina sosiaalisina huijauksina. Käyttäjää voidaan esimerkiksi lähestyä sähköpostilla esittäytyen pankin yhteyshenkilöksi ja pyytää tekaistulla syyllä käyttäjää luovuttamaan verkkopankkinsa käyttöön tarvittavat tunnukset. Suuri osa käyttäjistä pystyy tunnistamaan tämän tyyppiset huijaukset, mutta koska huijauksen laaja jakelu on helppoa, erehtyy joku vastaanottajista helposti astumaan hänelle asetettuun ansaan. [9.]

Käyttäjän salasanan voi saada haltuunsa epärehellisesti myös seuraamalla tai puuttumalla tiedonsiirtoon. Tämän tyyppinen hyökkäys vaatii pääsyä käsiksi verkkoliikenteeseen. Perinteisen kaapeleihin perustuvan tietoverkon kohdalla tämä on verrattain hankalaa koska verkkoon täytyy kytkeytyä fyysisesti. Nykypäivänä varsin yleiset langattomat tietoverkot ovat kuitenkin muuttaneet tilannetta oleellisesti. Jos käyttäjän tunnistetietoja siirretään suojaamattoman tai heikosti suojatun yhteyden yli, salasanan kaappaaminen verkkoliikenteestä on mahdollista helpohkosti. [8.]

Myös tunnistamiseen käytetty järjestelmä on alttiina hyökkäyksille. Lähtökohtaisesti salasanoista tulee säilyttää järjestelmän tietokannassa vain yksisuuntaisen tiivisteen tulos. Tiivisteiden käyttäminen selkokielisten tai symmetrisesti salattujen salasanojen sijasta tarkoittaa, että lähtökohtaisesti käyttäjän valitsemaa salasanaa ei voi palauttaa tietokannan tietojen perusteella, mutta salasanan vastaavuus voidaan todentaa. Käytännössä salasanat pystytään kuitenkin murtamaa rajallisessa ajassa brute-force-menetelmällä. Niinpä salasanatietokannan päätyminen ulkopuolisen tahon haltuun tarkoittaa käytännössä salasanojen suojausmerkityksen häviämistä ja siten salasanat tulisi mitätöidä ja vaihtaa välittömästi.

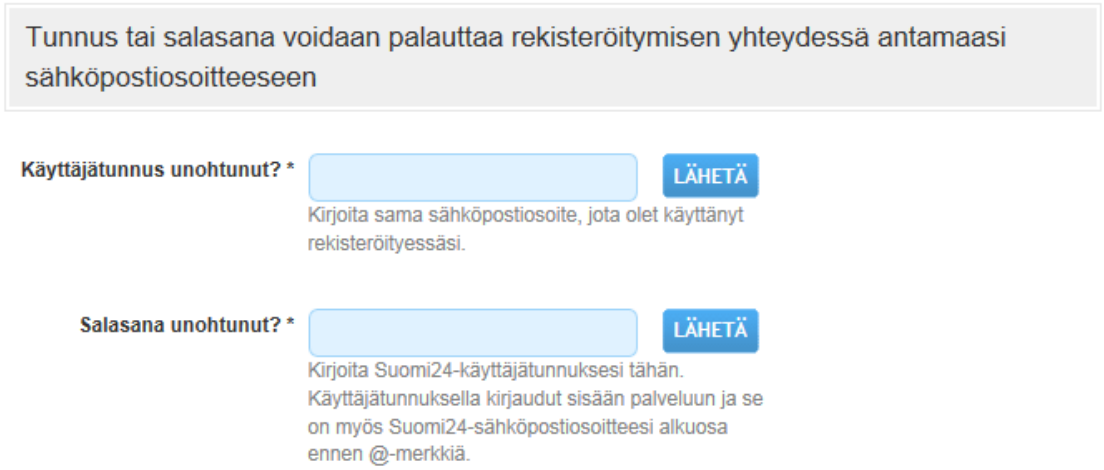
Vielä kriittisempi on tilanne, jossa ylläpito-oikeuksin varustettu tunnus on joutunut onnistuneen hyökkäyksen kohteeksi ja hyökkääjä on saavuttanut pääsyn järjestelmään. Riippuen järjestelmän tietoturvavaatimuksista tämä voi johtaa järjestelmän käyttökelvottomuuteen ja tarpeeseen luoda järjestelmä uudelleen tyhjästä. Vähimmillääkin vaatimuksena on kaikkien järjestelmään liittyvien salasanojen vaihtaminen. [8.]

Tässä kappaleessa esitettyjä tietoturvaongelmia kohtaan voi pyrkiä suojautumaan. Ensinnäkin tunnistetietojen siirto tulee suorittaa suojatun yhteyden yli. Lähtökohtaisesti jokaisen verkkoyhteyden suojaaminen olisi eduksi, mutta koska tähän ei voida luottaa, kannattaa siirtotie tunneloida. Väärinkäytöksiä voidaan ehkäistä myös lukitsemis- ja vanhenemiskäytännöillä. Tärkeää on myös käyttäjien kouluttaminen turvallisten salasanojen valitsemiseen. Hyvän salasanan tunnuspiirteisiin kuuluvat riittävä monipuolisuus, järjestelmäkohtainen uniikkius ja riittävän lyhyt vaihtoväli. Tunnuksia hallinnoivan tahon on lisäksi pyrittävä muodostamaan sopivan tasapainoinen määritelmä turvallisuuden ja käytettävyyden väliltä. Liiallisuuksiin menevät vaatimukset salasanojen suhteen aiheuttavat helposti niiden pitämistä saatavilla muistiinkirjoitettuina sekä turhia unohtamisia. [8.]

Unohtuneiden salasanojen palauttaminen

Yksi salasanoihin liittyvä ongelma on ihmisten taipumus unohtaa salasanansa. Salasanojen runsas määrä ja toisaalta vaatimus vaihtaa niitä säännöllisesti aiheuttaa monelle vaikeuksia muistaa kaikki salasanansa. Usein salasana unohtuu myös esimerkiksi loman aikana, kun salasanaa vaativia palveluita ei tule käytettyä säännöllisesti. Tämä aiheuttaa katkoja palveluiden käyttämiseen ja uusien salasanojen luominen kuormittaa palveluita tukevia henkilöitä.

Unohtuneiden salasanojen palauttamiseksi on olemassa erilaisia itsepalvelu-ratkaisuja. Useissa Internet-palveluissa käyttäjätilin tietoihin on tallennettuna käyttäjän sähköpostiosoite. Käyttäjän unohtaessa salasanansa tätä tietoa voidaan hyödyntää toimittamalla kyseiseen sähköpostiosoitteeseen tarvittavat tiedot (kuvassa 2 on lomake tietojen pyytämiseksi) uuden salasanan luomiseksi. Vastaavasti voidaan hyödyntää käyttäjän matkapuhelinnumeroa tekstiviestin lähettämiseksi.



Kuva 2. Unohtuneen salasanan palauttaminen

Tunnettuun sähköpostiosoitteeseen tai matkapuhelinnumeroon perustuvat salasanan palautusmekanismit ovat tilanteesta riippuen tietoturvaltaan hyväksyttävissä olevia. Nehän vaativat salasanaa palauttavan henkilön saavan haltuunsa käyttäjän puhelimen tai pääsevän lukemaan tämän sähköposteja. Sen sijaan ongelmallisempia ovat niin sanottuihin turvakysymyksiin perustuvat palautusjärjestelmät. Niissä käyttäjä on etukäteen vastannut häntä koskeviin kysymyksiin. Salasanaa palauttaessa näitä kysymyksiä esitetään käyttäjälle ja hänen tulee vastata niihin oikein luodakseen itselleen uuden salasanan.

Kysymyslistoihin liittyy suuria ongelmia. Kysymyksien laatiminen on erittäin vaativaa. Kysymysasettelu tulisi olla sellainen, että käyttäjän vastaukset ovat ulkopuolisille vaikeasti selvitettävissä, yksiselitteisiä ja siten helposti muistettavia sekä pitkällä aikavälillä pysyviä. Entistä haastavammaksi kysymysten käytön tekee sosiaalinen media, jossa ihmiset jakavat avoimesti tietoja itsestään.

3.2 Kertakäyttösalasanat ja varmenteet

Kertakäyttösalasanat ja varmenteet poikkeavat salasanoista sikäli, että niihin liittyy jokin käyttäjän hallussa oleva tunnistamiseen käytettävä esine. Tällaiseksi esineeksi voidaan määritellä muun muassa erilaiset salasanageneraattorit, varmenteen sisältävät muistit tai vaikkapa matkapuhelimet. [10.]

Yleisesti erillisestä tunnistukseen käytettävästä välineestä käytetään nimitystä ”token”. Sillä tarkoitetaan itsenäistä laitetta, joka kytketään tietokoneeseen tai jonka omalta

näytöltä näkyvä tieto syötetään tietokoneeseen tunnistuksen suorittamiseksi. Token sisältää useimmiten joko varmenteen tai kertakäyttösalasanageneraattorin. Molemmille on tyypillistä ennalta määritelty korkeintaan noin 4 vuoden mittainen elinkaari. Niin ikään käyttäjän haltuun luovutettavien tunnisteiden haittapuolena on tunnisteiden luomisen vaikeus. [7.]

Varmenne pohjaiseen tunnistamiseen liittyy useimmiten turvalliseen tiedon taltioimiseen käytetty väline, kuten USB-muisti tai älykortti. Muistivälineitä käytetään PKI-järjestelmän tuottamien varmenteiden taltioimiseen, käytännössä varmenteet ovat taltioituna muistivälineille suojatussa muodossa. Varmenne saadaan käyttöön erillisen ohjelmiston ja henkilökohtaisen PIN-koodin kautta. Älykortin tapauksessa vaaditaan lisäksi kortin lukemiseen soveltuva lukulaite, USB-muistille soveltuva USB-portti löytyy sen sijaan nykyisin lähes kaikista tietokoneista. [7.]

Varmenteita pidetään yleisesti luotettavana todentamiskeinona. Niitä voidaan hyödyntää käyttäjätunnistuksen lisäksi laajasti muun muassa viestien salaamiseen tai dokumenttien käyttöoikeuksien hallintaan. Varmenteiden käyttöönotto vaatii kuitenkin joko ulkopuolisen varmentajan käyttämistä tai oman PKI-järjestelmän käyttöönottamista. Ulkoisen varmentajan myöntämät sertifikaatit ovat käytettävissä myös oman organisaation ulkopuolella ja niiden käyttöönotto on verrattain nopeaa, mutta etenkin suurilla käyttäjämäärillä kustannukset kohoavat pitkällä aikavälillä helposti suuriksi. Vastaavasti oman PKI-järjestelmän käyttöönotto on asiallisesti toteutettuna hitaampi ja aloituskustannuksiltaan huomattavasti kalliimpi ratkaisu.

3.3 Biometriset tunnisteet

Biometriset tunnisteet perustuvat jonkin käyttäjän piirteen tai ominaisuuden tunnistamiseen. Biometrisen tunnistamisen etuna on tunnisteen yksilöllisyys ja se, että tunniste kulkee aina tunnistettavan henkilön mukana. Haluttaessa biometrisellä tunnistamisella on saavutettavissa liki täydellä varmuudella uniikit tunnisteet, jotka täsmäävät vain yhteen henkilöön. [7.]

Valitettavasti biometriseen tunnistamiseen liittyy myös paljon ongelmia. Ensimmäinen ongelma on tunnistamiseen tarvittavat laitteistot ja ohjelmistot. Käytännössä tunnistamista varten jokaisesta käytetystä päätelaitteesta tulee löytyä erillinen laitteisto ohjel-

mistoineen tunnisteiden lukemista varten. Toinen merkittävä ongelma liittyy tunnisteiden keräämiseen eli käyttäjien rekisteröimiseen. Jotta käyttäjä voidaan jatkossa tunnistaa, on hänestä ensin tallennettava tulevaa vertailua varten näyte tunnistukseen käytettävästä ominaisuudesta. Rekisteröinnin vaatima aika ja siihen mahdollisesti liittyvä paikkasidonnaisuus ovat yksi rasite. Toinen ongelma muodostuu tallennettavan tunnisteen sisällöstä. Tunnistustekniikasta riippuen rekisteröintivaiheessa kerätyistä tiedoista saattaa ilmetä henkilökohtaisia tietoja, kuten sairauksia tai vaikkapa käynnissä oleva raskaus. [8.]

Oman ongelmansa muodostaa myös tunnistettavan henkilön piirteiden muuttuminen ajansaatossa ja piirteiden vaihtelut myös lyhyemmällä aikavälillä. Esimerkiksi sormenjälkeen perustuvaa tunnistamista vaikeuttavat sormenjälkien tilapäiset vauriot sekä lämpötilan ja kosteuden vaihtelut. Sormenjälkiin ja useisiin muihin biometrisiin tunnisteisiin liittyy rasitteena myös fyysinen kosketus tunnistusprosessin aikana. [8.]

Biometrisen tunnistamisen tunnettuus on kasvamassa biometrisen passin käyttöönoton seurauksena. Biometrinen passi sisältää mikrosirun jolle on talletettuna henkilön kasvokuva ja sormenjäljet [11]. Nykyisin käytössä oleva standardi sallii myös iiriksen käytön tunnisteena. Iiris ei kuulu tällä hetkellä Euroopan unionin asetuksen määräämin tunnisteisiin [12]. Se olisi kuitenkin erinomainen lisä tunnistetietoihin, sillä iiris pysyy liki muuttumattomana ihmisen eliniän läpi. Sen lukeminen ei myöskään vaadi fyysistä kontaktia eikä paljasta terveydentilaan liittyviä seikkoja [8].

Biometriseen tunnistamiseen kuuluviksi luetaan myös muun muassa äänensävyyn, allekirjoituksen dynaamisuuteen ja näppäimistön käyttötekniikan analysointiin perustuvat seikat. Biometriset tunnisteet yleisesti ja etenkin juuri luetellut ovat toimivuudeltaan vahvasti riippuvaisia tunnistamisen herkkyyden suhteen tehdyille valinnoille. Yleisesti voidaan todeta, että mitä varmemmin tunnistus halutaan tehdä, sitä suurempi on riski väärille hylkäyksille. Vastaavasti vaatimusten keventäminen johtaa helposti vääriin positiivisiin tunnistuksiin. [8.]

3.4 Katsaus markkinoilla oleviin vahvan käyttäjätunnistuksen tuotteisiin

Vahvan käyttäjätunnistamisen markkinat ovat kasvussa. Kasvua ajavat monet syyt. Niistä selkein on salasanojen heikkous. Tietokoneiden laskentatehon alati kasvaessa salasanojen järjestelmällinen arvuutteleminen käy yhä helpommaksi. Salasanalla suojattavalle identiteetille kuuluvien oikeuksien kriittisyydestä riippuen tyypillisen salasanan suojauskyky on välttävä tai heikko. Toisaalta erilaiset säädökset, vaatimukset ja standardit noteeraavat yhä laajemmin salasanoihin liittyvät ongelmat ja suosittelevat tai vaativat vahvempien tunnistamistapojen käyttämistä. Ongelmat korostuvat etäyhteyksien yhteydessä ja niitä koskevat säännökset ovat vastaavasti tiukempia. [13.]

Pienemmän mutta silti merkittävän muutospaineen luovat etenkin julkista verkkoa uhkaavat identiteettivarkaudet ja verkkourkinta. Toisaalta uudentyyppisillä tunnistamismenetelmillä pystytään myös ratkomaan muita salasanoihin liittyviä ongelmia. Useiden säännöllisesti vaihdettavien salasanojen keskeinen ongelma on ihmisten taipumus unohtaa salasanansa. Tämä aiheuttaa ylimääräisiä kustannuksia käyttäjien tukemiseen liittyen. Vahvan käyttäjätunnistuksen keinoin salasanat voidaan poistaa tai niiden vaatimuksia voidaan keventää. Useimmiten vahvan tunnistamisen yhteydessä salasanaksi riittää PIN-koodin tyyppinen lyhyehkö salasana. [13.]

3.5 RSA SecurID

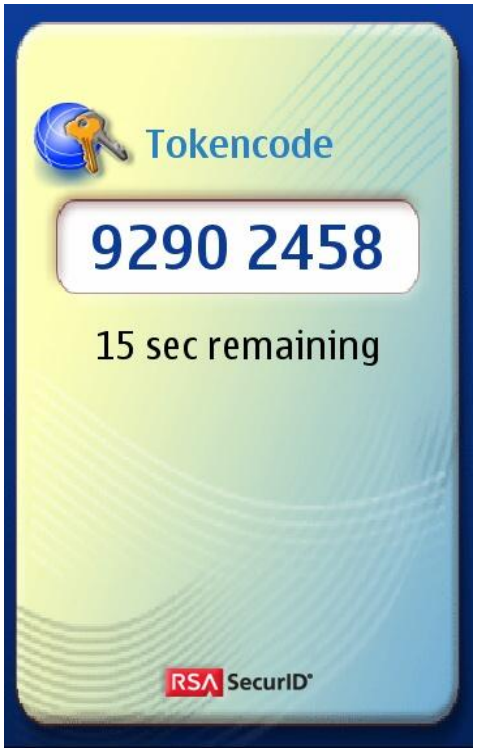
RSA, nykyisin EMC:n tietoturvaosasto, on ollut vuosien ajan markkinajohtaja kertakäyttösalasanojen markkinoilla. RSA:n SecurID-tuoteperhe on ollut erityisesti yritysten suosiossa. SecurID-tuoteperhe tarjoaa ratkaisun vahvan käyttäjätunnistuksen tuomiseksi niin VPN-yhteyksiin, langattomiin verkkoihin, Internet-sovelluksiin kuin käyttöjärjestelmiinkin. [14.]

Perinteisimmin vahva käyttäjätunnistus näkyy käyttäjälle annettavana kertakäyttösalasanageneraattorina (kuvassa 3). Avaimenperäksi soveltuva luo käyttäjälle uuden salasanan 60 sekunnin välein. Salasana näkyy laitteen omalta näytöltä. Salasanan luominen perustuu kullekin laitteelle yksilölliseen symmetriseen avaimeen. Tästä avaimesta luodaan käyttäjälle esitettävä salasana generaattorin sisäisellä algoritmilla. [14.]

Kuva 3. RSA SecurID -kertakäyttösalasanageneraattori

Viime vuosina tarjolle on tullut uudentyyppisiä ja edelleen kehitettyjä versioita salasanageneraattoreista. Kuvassa 3 esitetystä laitteesta on saatavilla myös USB-liittimellä varustettu versio. Näin laitteen ominaisuuksia on saatu laajennettua, ja se tukee sisäiselle muistille talletettuja varmenteita ja luodun kertakäyttösalasanan ohjelmallista lukemista. Näin saadaan käyttöön uusia tunnistamistapoja ja voidaan välttää tarve tunnistetiedon syöttämiseen käsin. [14.]

Käyttäjälle luovutettavassa yksinomaan tunnistamiseen käytettävässä laitteessa on ongelmansa. Se vaatii oman elinkaarenhallintansa ja aiheuttaa sitten ylimääräisiä kustannuksia. Lisäksi käyttäjä joutuu pitämään mukanaan erillistä laitetta. Näitä ongelmia ratkaisemaan on nykyisin tarjolla myös matkapuhelimeen pohjautuvia ratkaisuja. Nykyisin matkapuhelin kulkee ihmisten mukana lähes poikkeuksetta, joten älypuhelimeen asennettava kertakäyttösalasanoja generoiva ohjelmisto (kuvassa 4) on monesti oiva ratkaisu. [1.]



Kuva 4. RSA SecurID -kertakäyttösalasanageneraattori älypuhelimessa

Satunnaisempaan käyttöön vieläkin sujuvampi ratkaisu on SMS-pohjainen tunniste. Käyttäjän kirjautuessa palveluun omilla tunnuksillaan hänelle etukäteen määriteltyyn matkapuhelinnumeroon lähetetään tekstiviesti, joka sisältää kertakäyttösalasanan. Tällainen menettely ei vaadi käyttäjälle erikseen asennettavia lisälaitteita tai ohjelmistoja. Mikäli matkapuhelimesta löytyy tuki ominaisuudelle, voidaan viesti lähettää niin sanottuna flash-viestinä, joka ei tallennu puhelimeen vaan katoaa käyttäjän sulkiessa viestin. Haittapuolena sopimuksesta riippuen viestien lähettämisestä aiheutuu kustannuksia. [1.]

Kertakäyttösalasana voidaan toimittaa myös käyttäjän sähköpostiin. Näin vältytään salasanan toimittamiseen liittyviltä kustannuksilta sikäli, kun käyttäjällä on entuudestaan etäkäyttömahdollisuus sähköpostiinsa. Vahvan tunnistamisen kannalta ongelmalliseksi tilanne muodostuu, jos sähköposteihin pääsee käsiksi samalla salasanalla, jota kohdejärjestelmässä käytetään. Sen sijaan toimiva ratkaisu on esimerkiksi tilanne, jossa sähköpostit vastaanotetaan matkapuhelimella, jolloin on mahdollista suojata sähköpostien lukeminen salasanan lisäksi sidonnaisuudella kyseiseen matkapuhelimeen. Mahdollisesti lisäksi käytössä oleva web-pohjainen käyttöliittymä sähköpostiin voidaan tällöin suojata puhelimen kautta luettavalla kertakäyttösalasanalla.

3.6 Uhkakuvat

Laajasti käytettyihin teknisiin ratkaisuihin tai tuotteisiin liittyy aina kohonneita riskejä. Tällaisiin ratkaisuihin tai tuotteisiin kohdistuvat tietoturvaongelmat koskettavat lähtökohtaisesti laajaa käyttäjäkuntaa. Toisaalta laaja käyttäjäkunta houkuttelee etsimään tapoja murtaa kyseinen tietoturvan parantamiseen käytetty ratkaisu. RSA:n kohdalla tämä kävi osittain toteen maaliskuussa 2011. Hyökkääjä onnistui murtautumaan RSA:n järjestelmiin ja viemään SecurID-tuotteisiin liittyviä tietoja. [15.]

RSA ei ole tiedottanut tarkemmin siitä mitä tietoja hyökkäyksessä onnistuttiin viemään. Tämän hetkisten tietojen mukaan viedyillä tiedoilla saatetaan pystyä heikentämään SecurID-tuotteiden tietoturvaa [15]. Järjestelmä käyttää kirjautumisen vahvistamiseen käyttäjän käyttäjätunnusta, salasanaa ja generaattorin luomaa kertakäyttösalasanaa. Lisäksi yhdistelmään liittyy myös käytettävän palvelun osoite [16]. Näiden tietojen valossa ei ole välitöntä syytä olettaa kyseisen hyökkäyksen aiheuttaneen oleellista tietoturvan heikkenemistä.

Varotoimena on kuitenkin syytä kiinnittää huomiota salasanageneraattorien käyttötapoihin. Oleellista on suojata kertakäyttösalasanaa siihen liitettävällä kiinteällä salasanalla (tai PIN-koodilla), eli käyttää järjestelmää aidosti vahvaan käyttäjätunnistukseen. Lisäksi kiinteän salasanan osalta tulee noudattaa yleisiä salasanoja koskevia ohjeita. Salasanan pituudeksi suositellaan kahdeksaa merkkiä, ja salasana tulee vaihtaa välittömästi, jos on syytä epäillä sen joutuneen ulkopuolisten tietoon. [16.]

Julkisiin varmenteisiin liittyviä ongelmia

Julkisten varmenteiden käyttäminen pohjautuu varmentajaan kohdistuvaan luottamukseen. Ideaalitapauksessa kaikki varmentajat olisivat tuon luottamuksen arvoisia, ja kaikki myönnettävät varmenteet tarkistettaisiin huolellisesti. Niin ikään varmentamiseen liittyvä tekninen toteutus on pyritty suunnittelemaan turvalliseksi. Valitettavasti kummankaan lähtökohdan osalta tilanne ei ole tietoturvan kannalta aukoton. [17.]

Julkisten varmenteiden käyttö perustuu ennalta luotettavaksi määriteltyihin varmentajiin. Näiden luotettujen tahojen juurivarmenteet on asetettu luotettaviksi selaimissa ja käyttöjärjestelmissä. Kun jokin taho esittää varmenteen, jonka on allekirjoittanut luotettu taho, luotetaan myös varmenteen esittäjään. Varotoimena järjestelmään on luotu ominaisuus, jolla esitetyn varmenteen vastaanottaja voi tarkistaa varmenteen myöntäjältä varmenteen voimassaolon niin sanotusta sulkulistasta. [17.]

Oletuksena luotettaviksi asetettuihin tahoihin liittyy kaksi merkittävää ongelmaa. Kuka määrittelee kehen voidaan yleisesti luottaa? Useimmat selaimet luottavat oletuksena muun muassa ”China Internet Network Information Centerin” allekirjoittamiin varmenteisiin. Kyseinen laitos on Kiinan hallituksen alainen. Kun lisäksi tiedetään Kiinnan puuttuneen säännöllisesti maan sisäiseen verkkoliikenteeseen, näyttää luottamus hieman kyseenalaiselle. Toinen iso ongelma liittyy varmentajien liiketoimintaan. Yksittäisellä varmentajalla voi olla myönnettynä miljoonia maksullisia varmenteita. Jos varmentajan juurivarmenteen tietoturva murtuu (sillä on vaikkapa allekirjoitettu tahallisesti harhaanjohtavia varmenteita), kynnys juurivarmenteen mitätöimiseen on korkea. Näin siksi, että yksittäisten ongelmien takia mitätöity juurivarmenne vaatisi kaikkien varmentajan allekirjoittamien varmenteiden vaihtamisen uusiin. Lisäksi juurivarmenteen ennenaikainen mitätöiminen on raskas prosessi, koska se vaatii päivityksen viemisen käyttöjärjestelmiin ja selaimiin. [17.]

Ongelmia on myös sulkulistoissa ja niiden tarkistamisessa. Periaatteessa sulkulista (tai sen kehittyneempi versio ”online certificate status protocol” OCSP) on tehokas tapa yksittäisten varmenteiden nopeaan kuolettamiseen. Käytännössä ongelmaksi muodostuvat sulkulistojen ylläpitämiseen käytettyjen palvelinten säännölliset katkot. Jos varmennetta tarkastaessa vaadittaisiin aina varmistus sulkulistaa vasten, aiheuttaisivat sulkulistoja ylläpitävien palvelinten katkokset katkoja varmenteilla suojattuihin palveluihin. Yksittäiset katkot näkyisivät helposti miljoonille loppukäyttäjille. Tästä syystä varmennetta tarkistaessa hyväksytään yleisesti myös tilanne jossa palvelin ei pysty vastaamaan kyselyyn. [17.]

Varmenteisiin kohdistuvia puutteita tietoturvassa voidaan hyödyntää niin sanotussa ”man-in-the-middle”-hyökkäyksessä. Tällaisessa tilanteessa hyökkääjä asettuu asiakkaan ja palvelun väliin ja pystyy siten muokkaamaan tai uudelleen ohjaamaan liiken-

nettä. Varmenteiden pitäisi tarjota suoja tällaisia hyökkäyksiä vastaan, mutta mikäli hyökkääjä saa haltuunsa varmenteen, jolla se saa uskoteltua asiakkaalle olevansa tavoiteltu palvelu, on suoja menetetty. Hyökkääjä pystyy myös ohittamaan lisäturvana olevan sulkulistatarkastuksen, koska hän pääsee muokkaamaan myös kyselyn tuottamaa vastausta ja pystyy siten estämään kiellon perillepääsyn. [16.]

4 Vahva käyttäjätunnistus MOTP-AS-ohjelmistolla toteutettuna

Tämän työn käytännönosuudessa on tarkoitus toteuttaa vahvaa käyttäjätunnistusta hyödyntävä portaalityyppinen SSL VPN ratkaisu. Alustana VPN julkaisulle käytetään Microsoftin Unified Access Gateway -tuotetta. Itse vahvan käyttäjätunnistuksen toiminnallisuus tuodaan portaaliin MOTP-AS-ohjelmistolla (tarkemmin luvussa 4.2), joka on avoimen lähdekoodin yhteisön tuottama. Käyttäjille tarjotaan salasanageneraattoriksi avoimen lähdekoodin Mobile-OTP-projektin tuottama Java-pohjainen sovellus älypuhelimille.

Toteutettua ratkaisua on tarkoitus tarkastella suhteessa teoriaosuudessa käsiteltyihin seikkoihin. Oleellisena osana on myös käyttäjälle näkyvän toiminnallisuuden esittely. Lisäksi on tarkoitus pohtia SSL VPN -ratkaisun soveltuvuutta Trusteq Oy:n käyttöön.

4.1 Microsoft Unified Access Gateway 2010

Microsoft Unified Access Gateway 2010 (UAG) on verkonreunan pääsynhallintaan tarkoitettu tuote. Se pohjautuu Whale Communicationsin Intelligent Application Gateway -tuotteseen laajentaen sen ominaisuuksia. UAG tarjoaa mahdollisuuden toteuttaa hyvin Exchangeen ja Sharepointiin integroituvia julkaisuja. Lisäksi se tarjoaa VPN-ratkaisun, uuden DirectAccess-ominaisuuden ja entistä hienojakoisemman pääsynhallinnan. UAG yhdistää etäpalveluiden tuottamiseen tarvittavat komponentit yhteen tuotteeseen ja helpottaa siten järjestelmän ylläpitämistä. [17.]

UAG tarjoaa SSL-pohjaisen portaaliratkaisun Internet-sovellusten julkaisemiseksi julkiseen verkkoon. Portaalijulkaisun kautta on luontevaa julkaista palveluja ja sisältöä paitsi yrityksen työntekijöille, myös kumppaneille ja asiakkaille. Lisäksi UAG tukee uuden tyyppistä VPN-ratkaisua. DirectAccess-tekniikan tavoite on toteuttaa sisäverkkoa vastaavat ominaisuudet kaikkialta ja kaiken aikaa. Perinteisistä VPN-ratkaisuista poiketen asiakaskone muodostaa automaattisesti hallintatunnelin jo ennen käyttäjän kirjautumista. Tämä mahdollistaa koneen pääsyn taustajärjestelmiin ja vastaavasti koneen hallinnan etäyhteyden yli, aivan kuten kone olisi yrityksen omassa verkossa kaiken aikaa. Käyttäjän kannalta esimerkiksi ylläpidon palauttama salasana kelpaa suoraan kir-

jautumiseen koneelle ilman tarvetta tuoda konetta toimiston verkkoon. Ylläpidon kannalta asiakaskoneet on mahdollista päivittää myös etäyhteyksien yli ja esimerkiksi koneiden ja ohjelmistojen inventointi onnistuu riippumatta koneen sijainnista. [17.]

Käyttäjien tunnistamisen kannalta UAG tukee tämän hetken tärkeimpiä tekniikoita. Kolmannen osapuolen tuottein UAG:hen on mahdollista toteuttaa vahva käyttäjätunnistus. Se tukee muun muassa RADIUS-protokollaa, jonka kautta on helppoa laajentaa käyttäjätunnistus esimerkiksi kertakäyttösalasanoihin pohjautuvaksi. Lisäksi UAG mahdollistaa hienojakoisen pääsynhallinnan, jolla voidaan hallita käyttäjä- tai ryhmäkohtaisesti pääsyä julkaistuihin sovelluksiin. [17.]

Tietoturvan kannalta merkittävä ominaisuus on asiakaskoneiden luokittelu ja turvatarkastus. Se mahdollistaa yrityksen hallinnassa olevien koneiden erottamisen muista koneista. Tämän tiedon perusteella yrityksen koneilta avatuille yhteyksille voidaan sallia laajemmat oikeudet verrattuna hallitsemattomien koneiden kautta avattuihin yhteyksiin. Näin vaikkapa lentokentän web-kioskista avatulle yhteydelle voidaan määritellä huomattavasti tiukemmat säännöt (rajatummat palvelut, tiukempi käyttäjätunnistus, lyhyemmät istunnon aikakatkaisut). Niin ikään laajempien oikeuksien myöntämiseksi asiakkaalta voidaan vaatia turvatarkastus. Tämä tarkoittaa asiakaskoneella ajattavaa tarkistusta, joka raportoi UAG:lle muun muassa asiakkaan käyttöjärjestelmäversion, asennetut päivitykset ja virustorjunnan tilan. [17.]

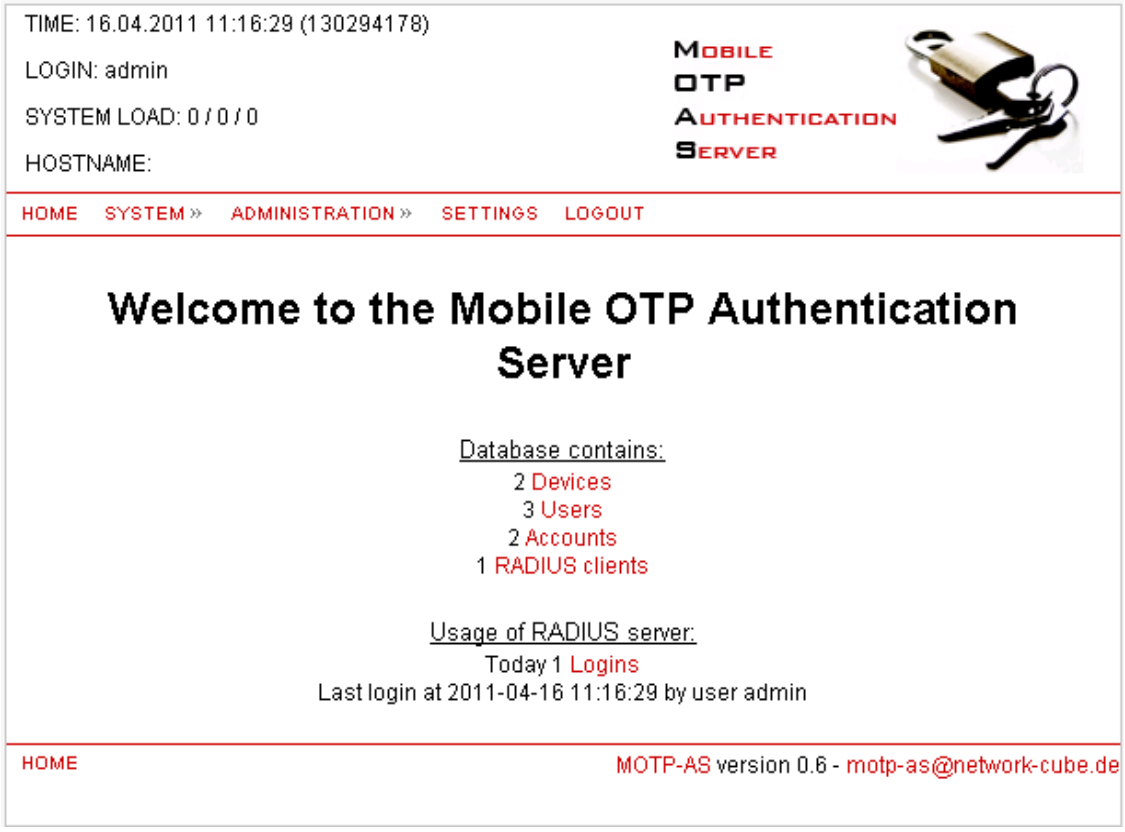
UAG on saatavilla joko laitteistona tai asennettavana sovelluksena. Se voidaan asentaa joko yksittäiselle palvelimelle tai useammalle koneelle ryppääksi kuormantasausta varten. Kappaleessa 4.3 käsitellään virtuaalikoneeseen asennettua ohjelmistoa.

4.2 MOTP-AS

MOTP-AS (Mobile OTP Authentication Server) on avoimen lähdekoodin ohjelmisto, joka sisältää RADIUS-protokollaa tukevan käyttäjätunnistuksen, SQL-tietokannan käyttäjä- ja laiteasetuksille sekä web-pohjaisen hallintakäyttöliittymän. Tässä työssä on käytetty openSUSE pohjaista Live CD:tä, jolta on mahdollista käynnistää kone suoraan valmiiksi asennettuun ympäristöön. Käytetty ohjelmisto ja asennusohjeet löytyvät osoitteesta http://motp-as.network-cube.de/index.php/home.

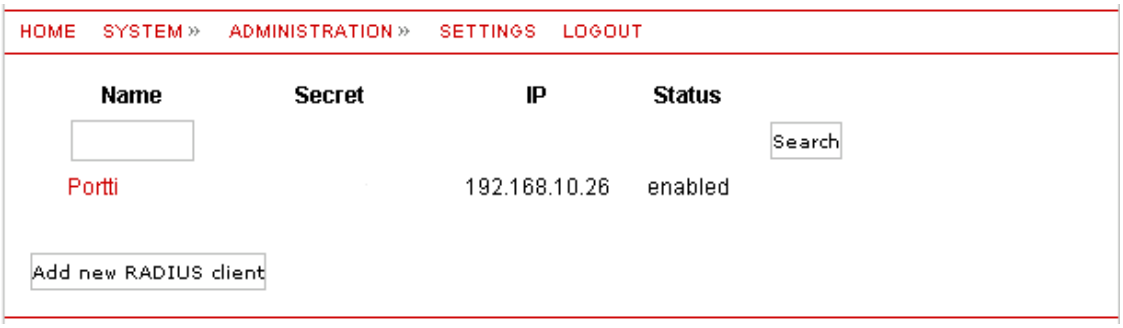
MOTP-AS palvelinta pystyy kokeilemaan live CD -ominaisuuden johdosta asentamatta sitä koneelle paikallisesti. Tässä työssä luodaan pysyvään käyttöön soveltuva ympäristö, joten asennus siirretään paikalliselle koneelle. Tämä tapahtuu käynnistämällä live CD ja käynnistämällä sen jälkeen ”live CD installer”. Asennusohjelma kysyy tarvittavat perustiedot (kuten verkkoasetukset) ja kopioi tarvittavat tiedostot palvelimelle. Uudelleen käynnistyksen jälkeen asennus viimeistellään vaihtamalla järjestelmän pääkäyttäjäsalasanat.

Asennettua palvelinta hallitaan selainkäyttöliittymän (esitetty kuvassa 5) kautta. Tämän työn kannata oleellista on tehdä sivuston kautta RADIUS-yhteyden, tunnistettavien käyttäjien ja tunnistukseen käytettävien laitteiden määritykset.



Kuva 5. MOTP-AS-hallintakäyttöliittymä

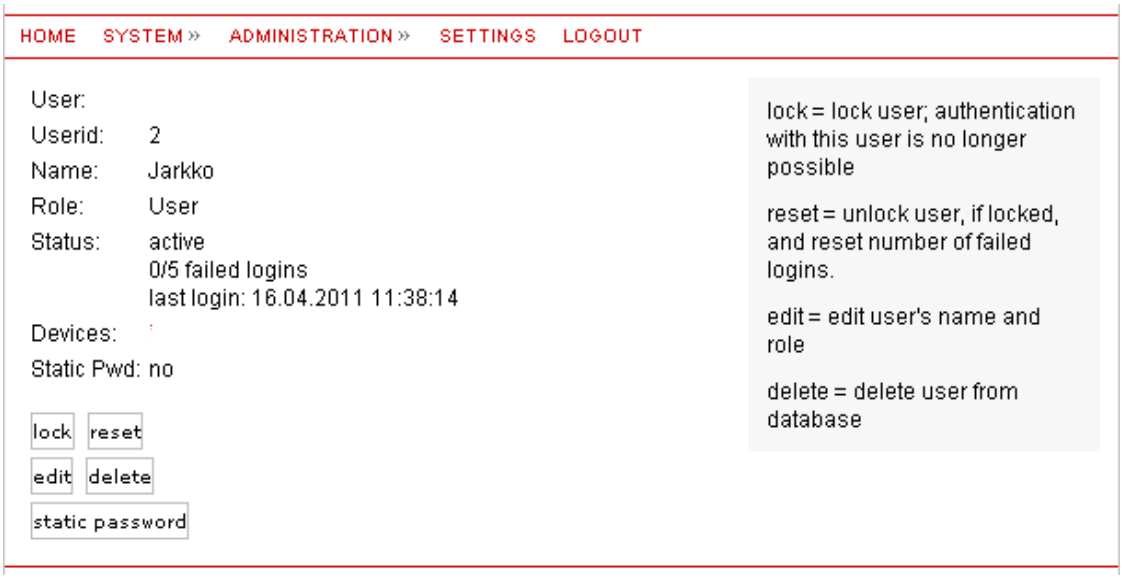
Liikenne RADIUS-asiakkaan ja -palvelimen välillä on suojattu. Suojaus perustuu molempiin päihin asetuttuun yhteiseen salaisuuteen ja palvelimelle kerrottuun asiakkaan IP-osoitteeseen. RADIUS-liikenteen sallimiseen tarvittavat asetukset on esitetty kuvassa 6.



Kuva 6. MOTP-AS RADIUS -asetukset

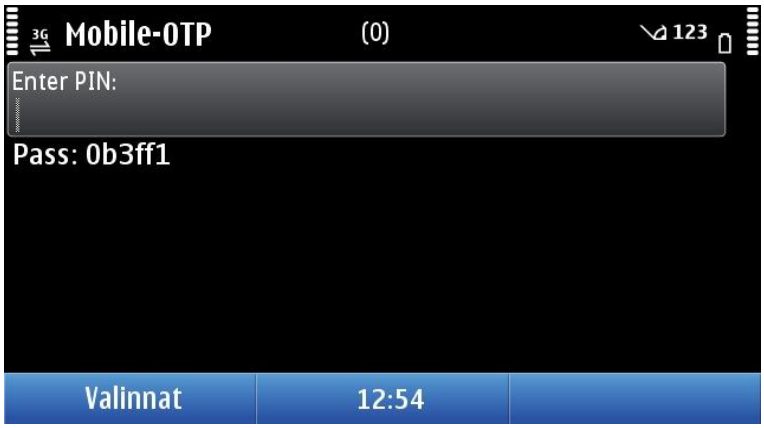
MOTP-AS käyttää sisäistä tietokantaa, johon tallennetaan tiedot tunnistettavista käyttäjistä. Tässä työssä tiedostetaan, että erillisen käyttäjätietokannan ylläpitäminen aiheuttaa ylimääräistä ylläpitotyötä. Toteutuksen pitämiseksi yksinkertaisena tässä työssä ei selvitetä mahdollisuutta käyttää julkaistavassa ympäristössä olevaa aktiivihakemistoa käyttäjätietokantana. Jotta kirjautumisvaiheessa syötettävä toimialueen käyttäjätunnus kelpaisi sellaisenaan myös MOTP-AS-palvelimelle, tulee järjestelmää käyttävien käyttäjien osalta luoda sen tietokantaan aktiivihakemistoa vastaavat käyttäjätilit.

Kuvassa 7 on esitetty yhden käyttäjän asetukset. Hallintakäyttöliittymä tarjoaa mahdollisuuden avata lukkiutuneet käyttäjätilit, muokata käyttäjätilejä tai asettaa käyttäjälle kiinteä salasana. Kiinteää salasanaa voidaan käyttää tilapäisesti tilanteessa, jossa salasanageneraattori ei ole käytettävissä. Kiinteä salasana suojataan joko rajoitetulla voimassaoloajalla tai rajoitetuilla kirjautumiskerroilla.



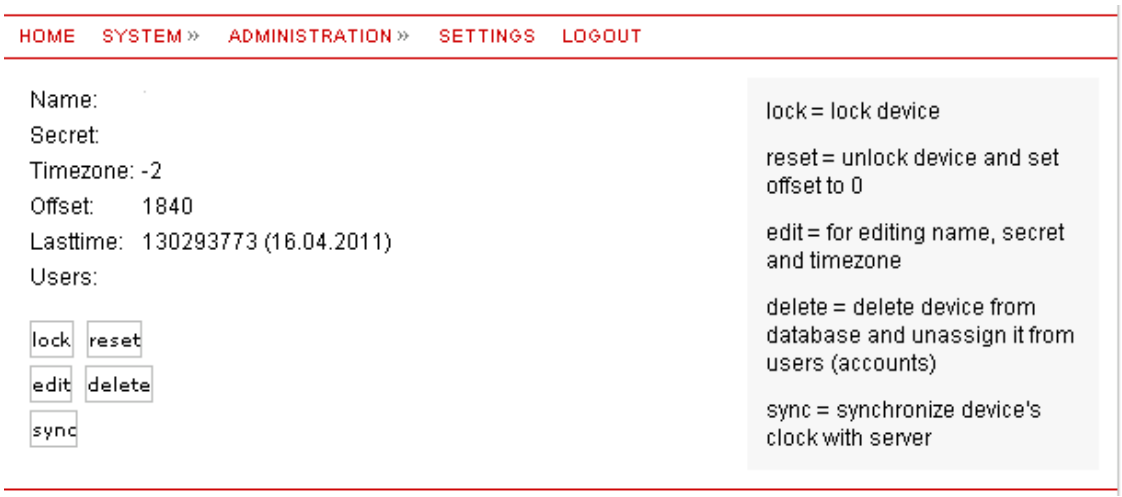
Kuva 7. MOTP-AS-käyttäjäasetukset

Tässä toteutuksessa käyttäjille tarjotaan Mobile OTP -projektin Java-pohjainen älypuhelinsovellus (kuvassa 8) kertakäyttösalasanojen luomiseksi. Sovellus luo käyttäjän syöttämän PIN-koodin, sovellukseen asennuksen yhteydessä syötetyn alustuskoodin ja kellonajan perusteella kertakäyttösalasanan. Salasana luodaan millä tahansa PIN-koodilla, mutta palvelin hyväksyy vain oikealla koodilla luodun salasanan.



Kuva 8. Mobile OTP -sovellus Nokia N8 -puhelimessa

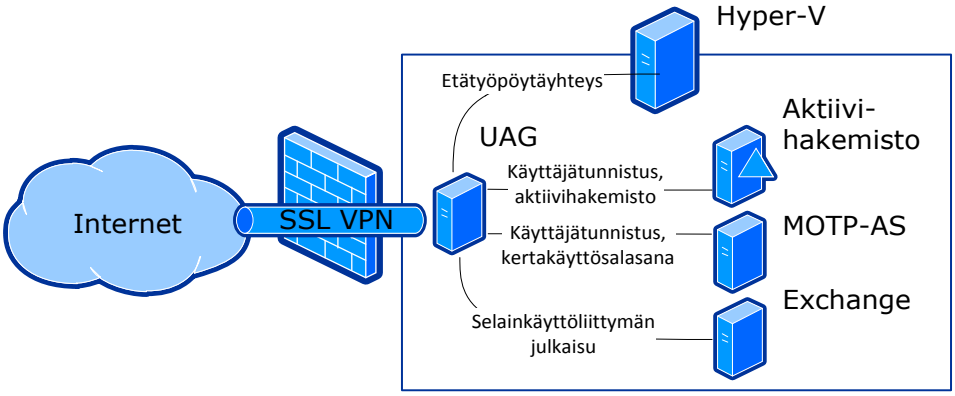
Käyttäjälle tarjottava Mobile OTP -salasanageneraattoria varten palvelimelle täytyy luoda laite ja ne tulee synkronoida keskenään. Kuvassa 9 on esitetty laitteen luomiseen liittyvät asetukset. Palvelimelle täytyy syöttää salasanageneraattorin alustukseen käytetty salaisuus ja puhelimen aikavyöhyke. Lisäksi puhelimen ja palvelimen kellonajat synkronoidaan keskenään ja laite liitetään aiemmin luotuun käyttäjätiliin.



Kuva 9. MOTP-AS-laitteen asetukset

4.3 Toteutettu ympäristö

Tässä työssä on toteutettu olemassa olevaan ympäristöön Microsoft UAG 2010 -tuotteeseen pohjautuva SSL VPN -ratkaisu, johon on liitetty MOTP-AS-käyttäjätunnistuspalvelin. MOTP-AS ja UAG 2010 -palvelimet ovat virtuaalisia. Toteutettu ympäristö on esitetty oleellisilta osin kuvassa 10.

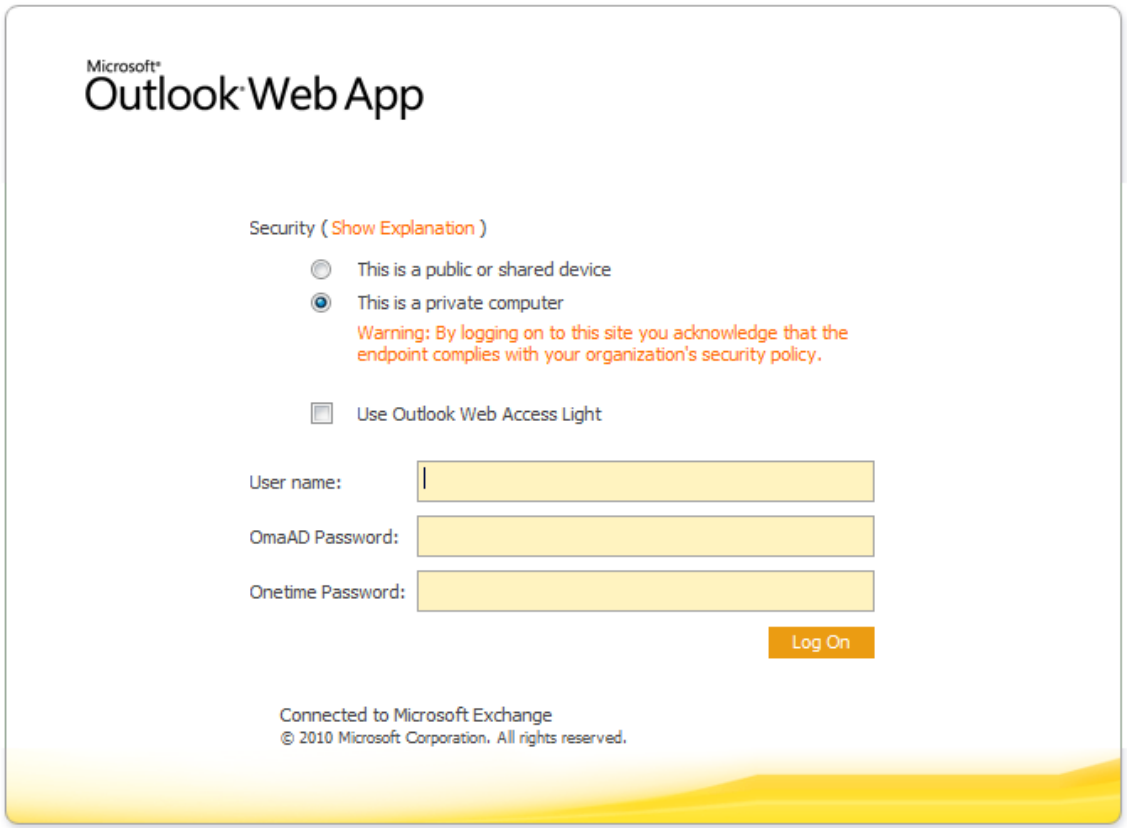


Kuva 10. Käytännöntoteutuksen ympäristö

Etäyhteyttä varten varatun julkisen IP-osoitteen portti 443 (HTTPS) on ohjattu UAG-koneen verkkokortille, joka on määritelty kuuluvaksi ulkoverkkoon. Liikenne julkaistuihin palveluihin ja käytettäviin tunnistuspalvelimiin on ohjattu sisäiseksi määritetyn verkkokortin kautta. Portaalille hankittu ulkopuolisen varmentajan allekirjoittama sertifikaatti on asetettu UAG ja Exchange palvelimille, jotta portaalin ja sen läpi julkaistun Outlook Web Appsin SSL-varmennus toimivat moitteettomasti.

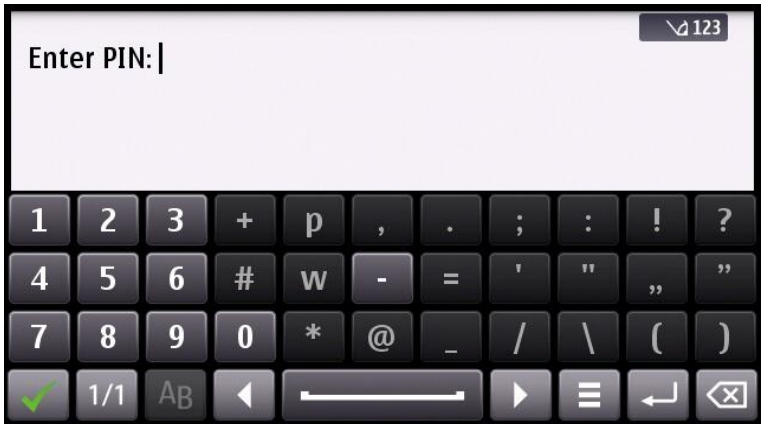
4.4 Toiminnallisuus

Toteutettu järjestelmä tarjoaa käyttäjälle suojatun pääsyn portaaliin, johon on julkaistu Outlook Web Apps, etätyöpöytäyhteys ja tiedostojako. Käytännössä prosessi resurssien käyttämiseksi alkaa avaamalla Internet-selain ja siirtymällä portaalin osoitteeseen. Portaalin kirjautumissivu (kuvassa 11) aukeaa SSL-suojatun yhteyden yli ja kysyy käyttäjän tunnistamiseen tarvittavat tiedot. Identiteettinä toimivaa käyttäjätunnusta käytetään sekä aktiivihakemistoa, että MOTP-AS-palvelinta vasten. Aktiivihakemiston osalta käyttäjältä pyydetään salasana ja MOTP-AS-palvelimen osalta kertakäyttösalasana.



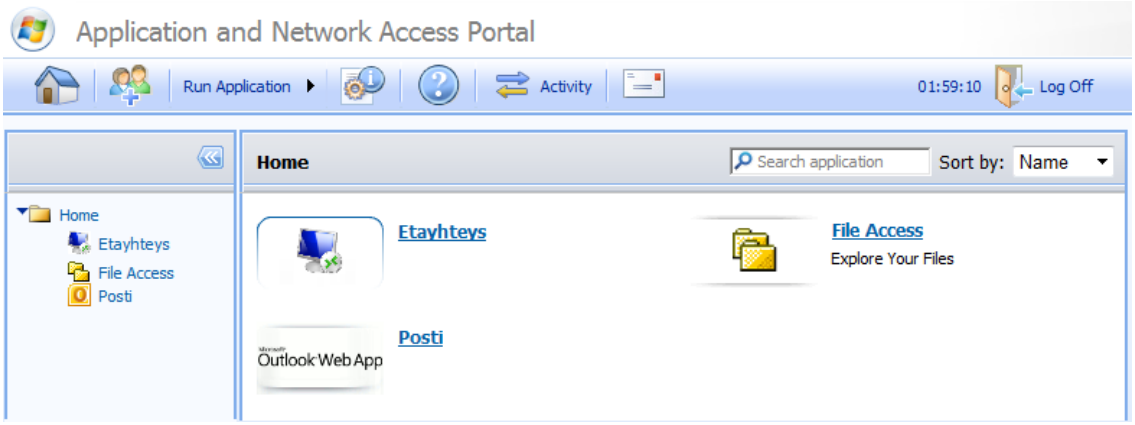
Kuva 11. Portaalin kirjautumissivu

Kirjautuakseen käyttäjän tarvitsee luoda itselleen kertakäyttösalasana. Tämä tapahtuu älypuhelimeen asennetulla MOTP-sovelluksella. Käyttäjän tulee syöttää sovellukselle (kuvassa 12) määrittelemänsä PIN-koodi, jonka perusteella kertakäyttösalasanan luodaan. Käyttäjä syöttää luodun kertakäyttösalasanan sille tarkoitettuun kenttään portaalin kirjautumisikkunassa.



Kuva 12. MOTP-kertakäyttösalasanan luominen

Kirjautumistietojen syöttämisen jälkeen tiedot varmennetaan tunnistuspalvelimien tietoja vasten. Mikäli tiedot hyväksytään, saa käyttäjä eteensä portaalin kotisivun (kuvassa 13), josta hän pääsee käyttämään hänelle julkaistuja sovelluksia.



Kuva 13. UAG-portaalin kotisivu

5 Päätelmät

Vahva käyttäjätunnistus on yhä merkittävämmässä asemassa luottamuksellisten tietojen ja järjestelmien suojaamiseksi. Salasanojen käytettävyys heikkenee yhä tunnistusta vaativien järjestelmien yleistyessä vauhdilla. Samaan aikaan salasanojen luoma turva heikkenee paitsi käyttötottumusten johdosta, myös tietokoneiden laskentakyvyn kehityksen myötä.

Teknisesti valittavissa on useita erilaisia tapoja ratkaista vaatimus vahvasta käyttäjätunnistuksesta. Kaikkiin toteutustapoihin liittyy kuitenkin omat hyvä ja huonot puolensa. Niinpä ratkaisua suunnitellessa tulee kartoittaa hyvin tarpeet, joihin ratkaisua haetaan, tuntea ympäristö, johon ratkaisu ollaan toteuttamassa ja siihen mahdollisesti vaikuttavat säädökset. Suunnitteluvaiheessa on myös syytä katsoa tulevaisuuteen ja pyrkiä ennakoimaan myös tulevia tarpeita. Varsinaisen käyttöönoton ja käytön kannalta oleellisimpia kysymyksiä ovat ratkaisun tarjoama tietoturva, järjestelmän ylläpidettävyys, yhteensopivuus sekä käyttäjien kouluttaminen ja totuttaminen uusiin toimintamalleihin.

5.1 Saavutetut tulokset

Tämä työ on opinnäytetyöprojektin tuloksena syntynyt tiivis katselmus vahvan käyttäjätunnistuksen nykytilaan. Tässä katselmuksessa esitellään vahvan käyttäjätunnistuksen määritelmä sekä tekniset menetelmät ja tutustutaan niihin läheisesti liittyvien etäyhteyksien toteuttamiseen.

Teknisen taustan lisäksi tässä työssä esitellään käytännössä yksi vahvan käyttäjätunnistuksen toteutus. Esitetyn ratkaisun toteuttaminen ja testikäyttö toteutuksen jälkeen ovat osoittaneet ratkaisun toteutuskelpoiseksi ja toimivaksi. Käyttökokemuksen kannalta ratkaisu on ollut helppokäyttöinen ja varmatoiminen.

5.2 Työn ulkopuolelle rajatut kehityskohteet

Tämän työn rajauksessa on pyritty tiiviiseen ja ehjään kokonaisuuteen, jolla työn aiheesta pystytään välittämään selkeä kokonaiskuva. Tästä syystä työssä on vältetty liialliseen tekniseen syvyyteen meneviä yksityiskohtia. Näistä rajauksista johtuen tämä työ ei yksinään anna täysin kattavaa lähtökohtaa vahvan tunnistuksen tai etäyhteyksien eri osa-alueisiin.

Suurimmat puutteet käsittelyssä liittyvät kriittiseen ja analyyttiseen tietoturvallisuuden arviointiin. Lisäksi käytännöntoteutuksen osalta myös toteutuksen käytettävyyttä ja toteutettavuutta yritysympäristössä olisi syytä tutkia tarkemmin. Ratkaisujen tietoturvan huolellisempi arviointi vaatisi teknisen taustan syvällisempää kartoittamista. Samoin käytännön osuuden osalta olisi syytä pohtia avoimen lähdekoodin ohjelmiston käyttämisen mahdollisia vaikutuksia tietoturvaan. Käsittelemättä ovat jääneet myös ratkaisujen toimintavarmuuteen vaikuttavat tekijät kuten mahdollisuus toteuttaa järjestelmien eri vaiheet vikasietoisina.

5.3 Tulosten hyödynnettävyys

Tämän työn tuloksena syntynyt raportti soveltuu ensikatsaukseksi henkilölle, joka ei entuudestaan ole tutustunut vahvan käyttäjätunnistuksen ratkaisuihin. Työstä löytyy varmasti monelle lukijalle viitteitä omaan arkielämään ja käytössä oleviin työkaluihin. Mikäli tämä työ saa lukijansa ajattelemaan esitettyjen menetelmien ja niihin liittyvien ongelmien vaikutusta jokapäiväisessä käytössä olevien ratkaisujen toimintaan on työ saavuttanut tavoitteensa. Lisäksi tässä työssä esitellään saatavilla olevia tuotteita ja ratkaisuja etäyhteyksien ja vahvan käyttäjätunnistuksen toteuttamiseen.

Trusteqin käyttöympäristön kannalta työssä esitelty vahvalla käyttäjätunnistuksella toteutettu SSL VPN -ratkaisu tarjoaisi SSL VPN:lle tyypillisiä etuja, kuten hienojakoisen käyttäjäkohtaisen oikeuksien hallinnan. Lisäksi se toisi monipuolisemman mahdollisuuden rajata käytössä olevien pilvipalveluiden käytettävyyttä vain etäyhteyden kautta sallituksi. Vahva käyttäjätunnistus on tässä päivässä toimivan tietoturva-alan yrityksen peruslähtökohta jo uskottavuudenkin takia. Se on tosin toteutettavissa myös perinteisempään IPSec VPN -ratkaisuun. Käytännönosuudessa esitellyn MOTP-ohjelmiston

käyttöönotto on tuskin vaihtoehto. Tämä johtuu pääosin kertakäyttösalasanageneraattorien alustamiseen työläydestä verrattuna kumppaniyritysten tarjoamiin ratkaisuihin verrattuna ja avoimen lähdekoodin taustan herättämistä kysymyksistä tietoturvan osalta.

Lähteet

[1] Hämäläinen, Pertti. 2005. Tietokone 9/2005: Vahva käyttäjätunnistus. Verkkodokumentti. [http://www.tietokone.fi/lehti/tietokone_9_2005/vahva_kayttajatunnistus_2321]. Luettu 18.4.2011.

[2] Frankel, S., Hoffman, P., Orebaugh, A., Park, R. 7.2008. NIST Special Publication 800-113: Guide to SSL VPNs. Verkkodokumentti. [http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf]. Luettu 14.4.2011.

[3] VAHTI: Turvallinen etäkäyttö turvattomista verkoista (luku 4. Etäkäytön uhkat ja niiltä suojautuminen). 2.2003. Verkkodokumentti. [https://www.vahtiohje.fi/c/document_library/get_file?uuid=370c931e-fe24-4061-b5ac-91f3cc81e28d&groupId=10128]. Luettu 15.4.2011.

[4] Frankel, S., Kent, K., Lewkowski, R., Orebauagh, A., Ritchey, R., Shama, S. 12.2005. NIST Special Publication: Guide to IPSec VPNs. Verkkodokumentti. [http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf]. Luettu 14.4.2011.

[5] Vacca, John. 2009. Computer and Information Security Handbook (luku 30. Virtual Private Networks). Verkkodokumentti. [http://www.books24x7.com]. Luettu 9.4.2011.

[6] Strong Authentication at Fermilab (luku 1. Introduction to Strong Authentication at Fermilab). 9.2006. Verkkodokumentti. [http://www.fnal.gov/docs/strongauth/strong_auth.pdf]. Luettu 4.4.2011.

[7] Federal Financial Institutions Examination Council: Authentication in an Internet Banking Environment. 10.2005. Verkkodokumentti. [http://www.ffiec.gov/pdf/authentication_guidance.pdf]. Luettu 5.4.2011.

[8] Stewart, J., Tittel, E., Chapple, M. 2008. CISSP: Certified Information Systems Security Professional Study Guide, Fouth Edition (luku 1. Accountability and Access Control). Verkkodokumentti. [http://www.books24x7.com]. Luettu 9.4.2011.

[9] Kuivalainen, Jaakko. 28.10.2005. Nordean suomalaisasiakkaat phishing-hyökkäyksen kohteena. Verkkodokumentti. [http://www.digitoday.fi/tietoturva-/2005/10/28/nordean-suomalaisasiakkaat-phishing-hyokkayksen-kohteena/200516729/66]. Luettu 9.4.2011.

[10] PointSharp ID 3.1: Authentication Methods White Paper. 2009. Pointsharp AB.

[11] Poliisi: Passi. Verkkodokumentti. [http://www.poliisi.fi/poliisi/home.nsf/suomi/passi]. Luettu 16.4.2011.

[12] Sisäministeriö: Biometrinen passi. Verkkodokumentti. [http://www.intermin.fi/intermin/hankkeet/biometria/home.nsf/pages/596EE8B62C0D31ABC2256E52002ED3F6?opendocument]. Luettu 16.4.2011.

[13] Vazquez, Martha. An Overview and Competitive Analysis of the One-Time Password (OTP) Market. Verkkodokumentti. [http://www.rsa.com/products-/securid/marketing/11156_FS_RSA_OPT_WP_100510_MLW_r7.pdf]. Luettu 11.4.2011.

[14] RSA Solution Brief: RSA SecurID Two-factor Authentication. 2010. Verkkodokumentti. [http://www.rsa.com/products/securid/sb/10695_SIDTFA_-SB_0210.pdf]. Luettu 11.4.2011.

[15] Coviello, Arthur. 2011. Open Letter to RSA Customers. Verkkodokumentti. [http://www.rsa.com/node.aspx?id=3872]. Luettu 21.4.2011.

[16] CERT.FI: Tietoturvakatsaus 1/2011. 12.4.2011. Verkkodokumentti. [http://www.cert.fi/katsaukset/2011/tietoturvakatsaus12011.html]. Luettu 15.4.2011.

[17] Goodin, Dan. 22.4.2011. The Register: How is SSL hopelessly broken? Verkkodokumentti. [http://www.theregister.co.uk/2011/04/11/-state_of_ssl_analysis/]. Luettu 15.4.2011.

[18] Implementing Forefront Unified Access Gateway 2010, Module 1: Forefront Unified Access Gateway Overview. 6.2010. Verkkodokumentti. [http://go.microsoft.com/?linkid=9735627]. Luettu 1.4.2011.